Protocol Datalekken

In het kader van gegevensuitwisseling in de geboortezorg

Sinds 1 januari 2016 geldt de meldplicht datalekken in de privacywetgeving. Deze meldplicht zorgt ervoor dat we bewuster omgaan met de opslag en beveiliging van persoonlijke gegevens. Privacy in de zorg is extra belangrijk omdat zorgaanbieders beschikken over veel gevoelige gegevens van hun cliënten en patiënten, zoals medische gegevens. De meldplicht houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra er een ernstig datalek is ontstaan. Daarnaast kan het zo zijn dat het datalek ook gemeld moet worden aan de mensen waarvan de gegevens zijn gelekt.
In dit protocol wordt beschreven wanneer er gesproken kan worden van een datalek en wanneer dit wel of niet gemeld moet worden bij de AP, aan cliënten/patiënten en aan andere zorgorganisaties.

Wat zijn persoonsgegevens?

Persoonsgegevens zijn alle informatie over een persoon. Het betekent dat deze informatie direct over iemand gaat, of naar deze persoon te herleiden is. Ook bestaan er bijzondere persoonsgegevens. Dit zijn gegevens die zo privacygevoelig zijn dat het grote impact op iemand kan hebben als deze gegevens worden gebruikt. Dit soort gegevens krijgen extra bescherming in de privacywetgeving. Gegevens over iemands gezondheid vallen onder de categorie “bijzondere persoonsgegevens”.

Wat is een datalek?

Bij een datalek gaat het om onterechte of onbedoelde toegang tot persoonsgegevens. Maar ook om het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens. Dit kan over gegevens gaan die in een systeem staan of op papier. Het kan bijvoorbeeld gaan over onbedoelde/ongewenste toegang tot het cliëntinformatiesysteem, een kwijtgeraakte USB-stick, gestolen laptop of een uitgeprint A4-tje met cliëntgegevens bij de printer laten liggen.
Een datalek kan op verschillende plekken ontstaan: in de praktijk/zorginstelling zelf of bij een andere praktijk/zorginstelling waarmee gegevens worden uitgewisseld.

Verwerkersverantwoordelijke vs. verwerker van gegevens

In het geval van Babyconnect schakelen organisaties HINQ in om persoonsgegevens te verwerken. In dit geval wordt HINQ de verwerker genoemd. Alle zorgorganisaties die HINQ inzetten zijn de verwerkingsverantwoordelijke.

Verwerkingsverantwoordelijke:

Je bent verwerkingsverantwoordelijke als je met jouw praktijk/zorginstelling bepaalt met welk doel de persoonsgegevens worden verwerkt en de manier waarop dit gebeurt. HINQ moet deze instructies volgen.

Verwerker:

Je bent verwerker als je persoonsgegevens verwerkt in opdracht van een andere organisatie. De persoonsgegevens worden niet voor eigen doeleinden gebruikt.

Meldplicht

Alle medewerkers van de praktijk/zorginstelling zijn verplicht een melding te doen van een datalek wanneer deze opgemerkt is. Mocht iemand in de praktijk/zorginstelling een datalek constateren of vermoeden, dan kan aan de hand van dit protocol bepaald worden welke stappen ondernomen moeten worden.

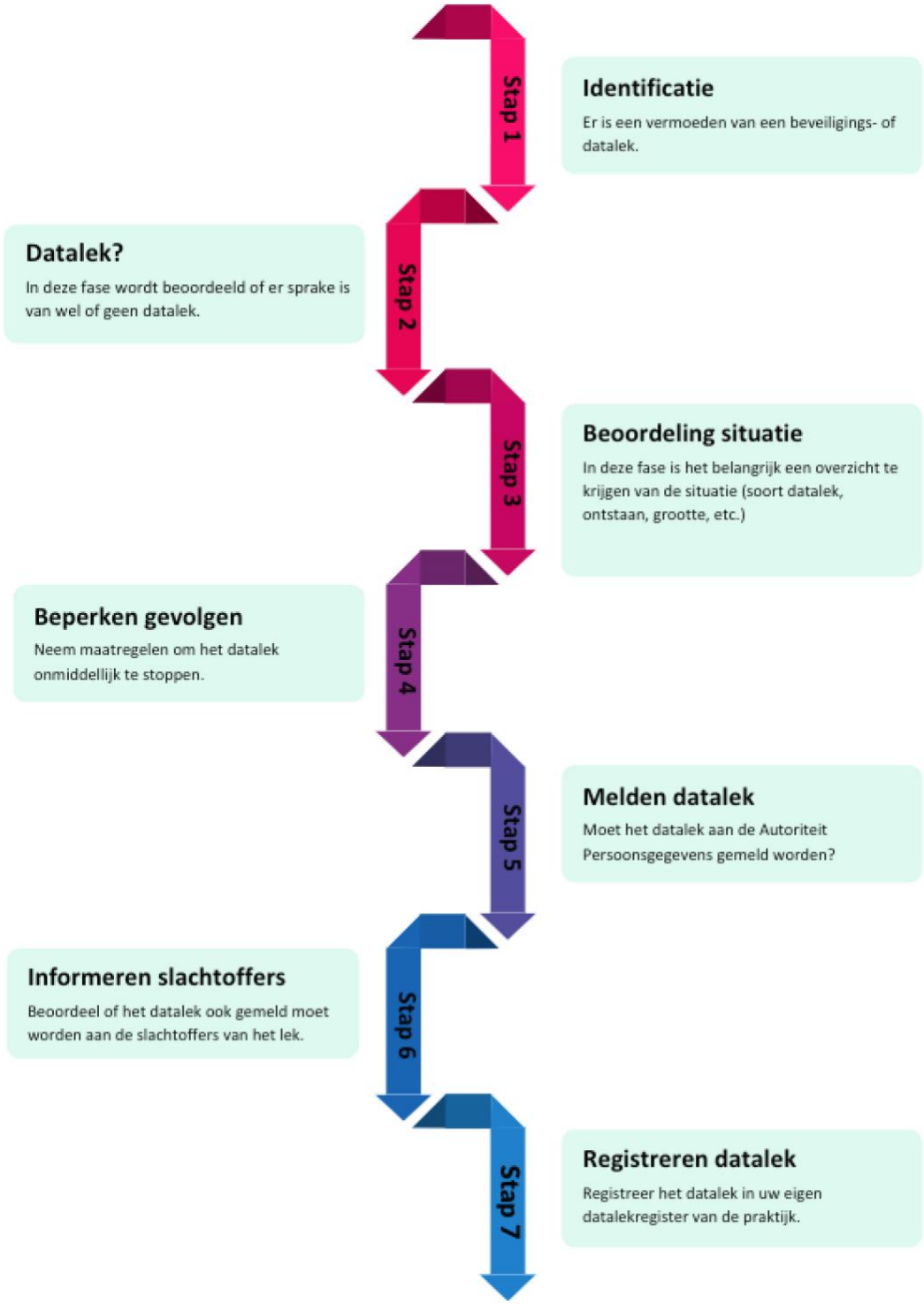
Verantwoordelijkheden in de praktijk/zorginstelling bij een datalek

- Alle medewerkers kunnen een datalek melden aan de leidinggevende of de collega die verantwoordelijk is voor privacy binnen de praktijk/zorginstelling.
- Het onderzoek naar de aard en ernst van het datalek wordt gedaan door de leidinggevende of de collega die verantwoordelijk is voor privacy binnen de praktijk/zorginstelling. Deze persoon zorgt ook voor de interne registratie van het datalek. Dit dient in afstemming te worden gedaan met de functionaris gegevensbescherming die betrokken is bij de praktijk/zorginstelling.
- De verwerkersverantwoordelijke zorginstelling is verantwoordelijk voor het melden van het datalek bij de AP. De persoon met privacy als aandachtsgebied maakt in samenwerking met de collega die het lek ontdekt heeft, wanneer dat nodig is, een melding bij de Autoriteit Persoonsgegevens.

Toepassing Babyconnect

Zoals eerder beschreven kan een datalek ontstaan wanneer er gegevens worden uitgewisseld met andere organisaties. Elke handeling met persoonsgegevens heeft een risico in zich. Daarom is het belangrijk nog bewuster met de veiligheid van deze gegevens om te gaan. Bij een datalek waarbij gegevens uitgewisseld zijn van de ene organisatie naar de andere, is het noodzakelijk zo snel mogelijk contact op te nemen met de functionaris gegevensbescherming van de andere organisatie. Wanneer er geen functionaris gegevensbescherming betrokken is, kan dit ook een verloskundige zijn die privacy/gegevensbescherming als aandachtsgebied heeft. Welke acties ondernomen moeten worden, staat verder in dit document beschreven.

De stappen:


Stap 1
Identificatie
Er is een vermoeden van een beveiligings- of datalek.
Stap 2
Datalek?
In deze fase wordt beoordeeld of er sprake is van wel of geen datalek.
Stap 3
Beoordeling situatie
In deze fase is het belangrijk een overzicht te krijgen van de situatie (soort datalek, ontstaan, grootte, etc.)
Stap 4
Beperken gevolgen
Neem maatregelen om het datalek onmiddellijk te stoppen.
Stap 5
Melden datalek
Moet het datalek aan de Autoriteit Persoonsgegevens gemeld worden?
Stap 6
Informeren slachtoffers
Beoordeel of het datalek ook gemeld moet worden aan de slachtoffers van het lek.
Stap 7
Registreren datalek
Registreer het datalek in uw eigen datalekregister van de praktijk.

In onderstaande alinea's wordt verdere toelichting gegeven op het stappenplan voor het omgaan met een datalek. Na de tekstuele uitleg is een beknopt stroomdiagram toegevoegd om onderste tekst toepasbaar te maken in de praktijk.

Stap 1: identificatie

Allereerst constateert een collega dat er een incident heeft plaatsgevonden dat er onterechte of onbedoelde toegang tot cliëntgegevens is geweest, of dat er ongewenst cliëntgegevens zijn vernietigd, verloren, gewijzigd of verstrekt. Het kan ook zijn dat er een vermoeden is dat dit gebeurd is.

Stap 2: beoordeling: wel of geen datalek?

In deze stap wordt beoordeeld of het beveiligingsincident een datalek is. Wanneer er bij de inbreuk geen persoonsgegevens verloren zijn gegaan of wanneer er redelijkerwijs uitgesloten kan worden dat er persoonsgegevens onrechtmatig zijn verwerkt, dan is dit geen datalek.
Wanneer er wél persoonsgegevens verloren zijn gegaan en/of er niet uitgesloten kan worden dat de persoonsgegevens onrechtmatig zijn verwerkt is dit wel een datalek.

Stap 3: zorg voor overzicht op de situatie

Om te weten welke vervolgstappen in gang gezet moeten worden, is het belangrijk om overzicht te krijgen. Dit overzicht creëer je gemakkelijk door onderstaande checklist in te vullen.

Checklist aan vragen voor het verhelderen van de situatie:

- Wat voor een soort datalek is het?

Inbreuk op	**Toelichting**
Vertrouwelijkheid	Persoonsgegevens zijn openbaar gemaakt of iemand heeft toegang tot gegevens die daar niet toe bevoegd is.
Integriteit	Persoonsgegevens zijn gewijzigd door iemand die daar niet voor bevoegd is.
Beschikbaarheid	De praktijk/zorginstelling heeft geen toegang meer tot eigen gegevens (bijv. door vernietiging).

- Wat is de oorzaak?
- Wanneer is het ontstaan? Is het nog steeds gaande?
- Hoe lang na het ontstaan van het datalek is het ontdekt? Hoe is het ontdekt?
- Wat voor soort persoonsgegevens zijn gelekt? Bijv. naam, adres, e-mailadres, medische gegevens.
- Hoeveel persoonsgegevens zijn er gelekt? Om hoeveel personen gaat het?
- Om wat voor groepen mensen gaat het? Bijv. klanten, cliënten.
- Hoeveel onbevoegden hadden of hebben toegang tot de gelekte persoonsgegevens?
- Heeft u zicht op wie die onbevoegden zijn? Is het waarschijnlijk dat de onbevoegden kwade bedoelingen hebben met deze gegevens?
- Heeft de praktijk vooraf maatregelen getroffen waardoor de gelekte persoonsgegevens ontoegankelijk zijn voor onbevoegden? Bijv. omdat de gegevens versleuteld zijn?

Stap 4: bepalen van schadelijke gevolgen datalek

Om de gevolgen van een datalek zoveel mogelijk te beperken is het noodzakelijk maatregelen te nemen om het te stoppen. Hoe u dat beperkt, leest u hier.

- Het datalek dient onmiddellijk stopgezet te worden
    - Neem hiervoor contact op met betrokken organisaties bij dit lek. Bijvoorbeeld in de volgende casus:
      Het ziekenhuis heeft gegevens ontvangen van een patiënt die niet bij hen zorg ontvangt. Neem dan direct contact op met de Functionaris Gegevensbescherming van het ziekenhuis om dit datalek te melden en te vragen dit lek te corrigeren door: gegevens te verwijderen. Controleer ook waar het verzenden van deze informatie fout is gegaan, is er in het eigen systeem iets verkeerd geregistreerd of is dit een fout door menselijk handelen. Zorg ervoor dat dit lek in de toekomst niet meer voor zal komen.
- Om negatieve gevolgen te beperken dient u maatregelen te nemen
  Voorbeelden:
    - Een laptop, tablet of telefoon op afstand wissen of versleutelen;
    - Een gepubliceerd bestand offline halen;
    - Een verkeerde ontvanger vragen om een bevestiging dat de gegevens uit een brief of e-mail zijn vernietigd.
    - De toegang tot een account blokkeren.
- Wanneer het eigen team er niet toe instaat is om zelf maatregelen te nemen, is het aan te raden professionele hulp in te schakelen. Bijv. van een ICT-bedrijf of van de leverancier van het systeem waar de cliëntdossiers in bijgehouden worden.

Stap 5: melden van het datalek aan de Autoriteit Persoonsgegevens?

In deze stap wordt bepaald of het noodzakelijk is om het datalek te melden aan de Autoriteit Persoonsgegevens (AP). Zo ja, dan moet dit binnen 72 uur (weekend/nacht telt ook mee). Of dit gedaan moet worden is afhankelijk van de impact van het datalek op de slachtoffers. Bij het bepalen van het risico van een datalek kijkt u naar de omstandigheden van het datalek. Soms is het risico heel duidelijk: medische dossiers zijn gelekt.

Factoren bij risico datalek:
<u>De aard van de inbreuk</u>
Zijn er gegevens gewist, gewijzigd of gelekt? (Bijv. het lekken van gegevens aan een onbevoegd persoon heeft andere gevolgen dan persoonsgegevens die gewist zijn).

<u>De aard en gevoeligheid van persoonsgegevens en hoeveelheid</u>
Hoe meer gegevens gelekt zijn, hoe groter het probleem is.
Hoe gevoeliger de gelekte gegevens, hoe groter het risico op schade.
Gegevens die een hoog risico hebben:

- Gegevens over gezondheid (ook wel bijzondere persoonsgegevens)
- Strafrechtelijke persoonsgegevens

<u>Het gemak waarmee personen kunnen worden geïdentificeerd</u>
Hoe makkelijker de gegevens te herleiden zijn naar een individu, hoe hoger het risico. Als gegevens zijn versleuteld is het risico een stuk lager. Gegevens die al openbaar beschikbaar zijn, hebben ook een lager risico.

De ernst van de gevolgen voor de slachtoffers
Kan het lek leiden tot financiële schade, lichamelijk en/of psychologisch leed? Dan kunnen er ernstige gevolgen zijn voor de slachtoffers.

Kenmerken van de onbevoegde ontvanger
Zijn er gegevens verstrekt aan een verkeerde ontvanger, maar kunt u objectief vaststellen dat deze ontvanger betrouwbaar is (bijv. beroepsgeheim)? Dan kan dit als een lager risico meegewogen worden. Hierbij is het noodzakelijk om een bevestiging van de betrouwbare ontvanger te krijgen dat de gegevens uit hun systeem weer zijn gewist.
Is niet bekend wie de gegevens inzichtelijk heeft gekregen, of is bekend dat er bewust is ingebroken op de gegevens, dan is er een hoog risico op misbruik van de gegevens.

Bijzondere kenmerken van de persoon
Zijn de slachtoffers kinderen, ouderen of mensen met een beperking, dan betekent dit een verhoogd risico op de omvang van de impact.

Bijzondere kenmerken van uw praktijk
Risico's van datalekken bij zorg-gerelateerde instellingen zijn groter dan bij een mailinglijst van een krant.

Aantal slachtoffers
Hoe meer slachtoffers, hoe groter de gevolgen. Maar een inbreuk voor 1 persoon kan alsnog ernstige gevolgen hebben.

Wel of niet melden datalek bij Autoriteitpersoonsgegevens:
Je beoordeelt zelf of het datalek moet worden gemeld bij de AP. Twijfel je? Dan kun je het beste het zekere voor het onzekere nemen en het datalek wel melden. Een datalek dient altijd binnen **72 uur** gemeld te worden aan de AP. Avond, nacht en weekend tellen hierin mee.

In sommige gevallen kan er sprake zijn van een datalek met medische gegevens, maar hoeft het alsnog niet aan de AP gemeld te worden. Dat is het geval in het volgende voorbeeld:
Vanuit de verloskundepraktijk worden onterecht medische gegevens gedeeld met een gynaecoloog in het ziekenhuis. De gynaecoloog heeft bevestigd dat de gegevens niet (meer) in het ziekenhuis opgeslagen zijn. Dit datalek hoeft niet gemeld te worden aan de AP doordat de gynaecoloog ook werkt met een beroepsgeheim.

Stap 6: wel of niet informeren slachtoffers datalek
Moet het datalek niet gemeld worden bij de AP, dan hoef je het datalek ook niet te melden aan de slachtoffers. Slachtoffers dienen geïnformeerd te worden als het lek een hoog risico voor hun persoonlijke gegevens, levenssfeer en vrijheden oplevert. Dit beoordeel je zelf op basis van de risico-inschatting uit stap 5.

Als je het datalek wel meldt aan de slachtoffers, dan dienen zij met het volgende geïnformeerd te worden:
- Wat er is gebeurd;
    - Welke gegevens?
    - Zijn gegevens bij onbevoegde(n) terecht gekomen?
    - Is er geen toegang meer tot de gegevens?
    - Zijn de gegevens verloren gegaan?
- Wat de waarschijnlijke gevolgen zijn;
    - Is alleen de privacy geschonden of is er ook sprake van lichamelijke schade?
    - Zijn de gegevens in handen van kwaadwillenden (hackers)? Kan het slachtoffer als gevolg hiervan phishingmails ontvangen?
    - Zijn de persoonsgegevens inmiddels teruggestuurd of vernietigd door de partij die de gegevens onterecht heeft ontvangen?

- Welke maatregelen er getroffen zijn;
    - Is hiervoor een externe partij om advies gevraagd?
    - Kan het lek niet meer voorkomen?
- Wat kunnen de slachtoffers zelf nog doen;
    - Wachtwoorden wijzigen?
    - Alertheid op eventuele fraude
- Waar de slachtoffers terecht kunnen met vragen;
    - Geef hierbij contactgegevens van de collega die dit als portefeuille heeft

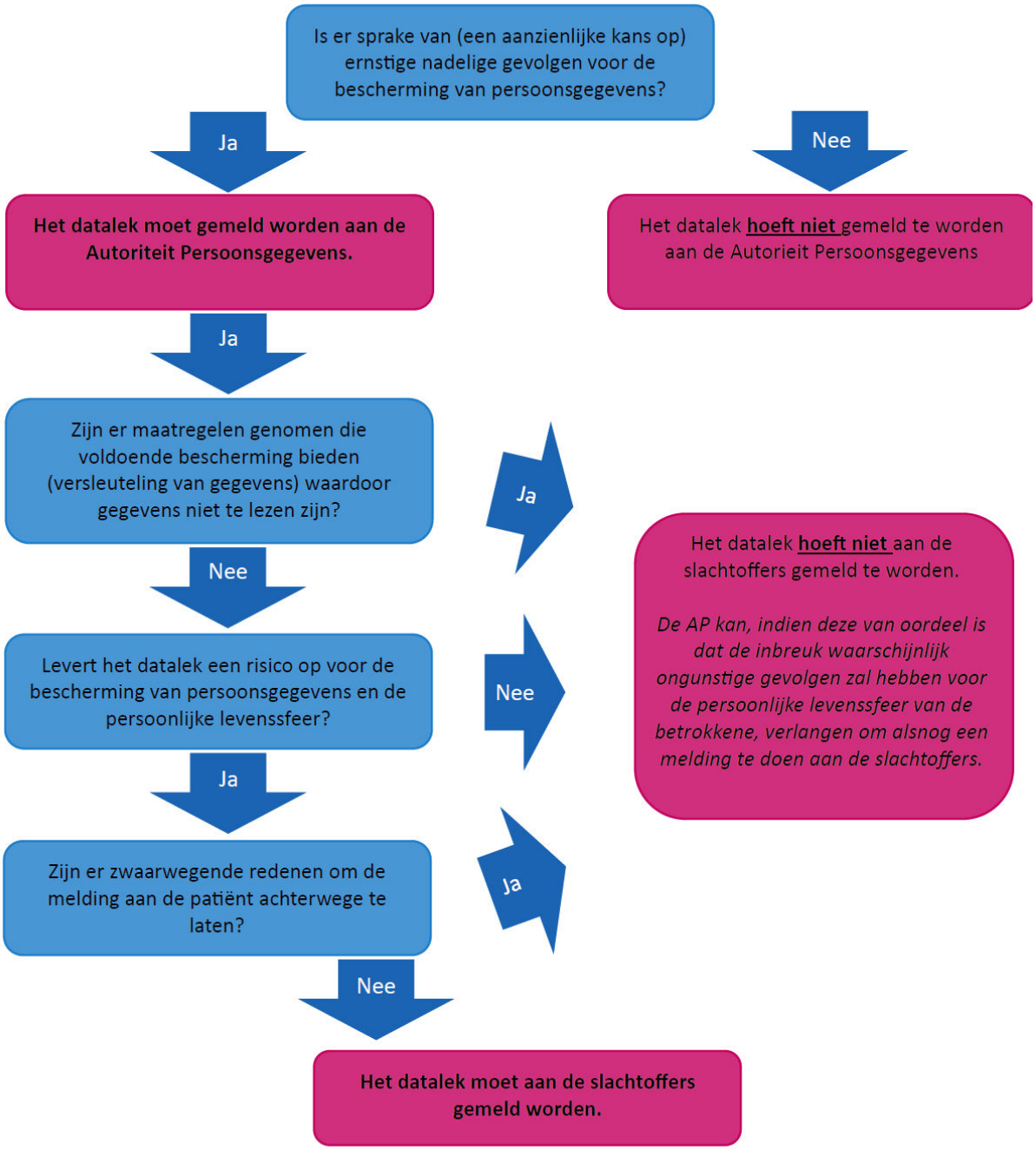
Stap 7: registreren datalek in het datalekregister

Elke praktijk/zorginstelling is verplicht een datalekregister bij te houden. In dit register staan datalekken die hebben plaatsgevonden binnen uw organisatie. Dit zijn ook de datalekken die niet gemeld worden aan de AP of aan de slachtoffers.

De vorm van dit register bepaal je zelf, zolang er in ieder geval de volgende informatie in terugkomt:

- Feiten over het datalek;
    - Oorzaak
    - Wat is er gebeurd?
    - Om welke persoonsgegevens gaat het?
- Gevolgen van het datalek;
- Corrigerende maatregelen die zijn genomen.

In het stroomschema op de volgende pagina staat concreet welke acties ondernomen moeten worden in welke fase wanneer er geconstateerd is dat er sprake is van een datalek.


Is er sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens?
Ja
Nee
Het datalek moet gemeld worden aan de Autoriteit Persoonsgegevens.
Het datalek hoeft niet gemeld te worden aan de Autorieit Persoonsgegevens
Ja
Zijn er maatregelen genomen die voldoende bescherming bieden (versleuteling van gegevens) waardoor gegevens niet te lezen zijn?
Ja
Het datalek hoeft niet aan de slachtoffers gemeld te worden.
De AP kan, indien deze van oordeel is dat de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, verlangen om alsnog een melding te doen aan de slachtoffers.
Nee
Levert het datalek een risico op voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer?
Nee
Ja
Zijn er zwaarwegende redenen om de melding aan de patiënt achterwege te laten?
Ja
Nee
Het datalek moet aan de slachtoffers gemeld worden.

Het datalekkenprotocol in relatie tot Babyconnect

Beoordeel of HINQ of andere praktijken/zorginstellingen geïnformeerd moeten worden

In deze situatie zijn er drie verschillende mogelijkheden.

1. Het datalek is ontstaan bij HINQ
2. Het datalek is ontstaan bij een praktijk/zorginstelling zonder dat er gegevens van andere zorginstellingen bij betrokken zijn
3. Het datalek is ontstaan bij een praktijk/zorginstelling waarbij er wel gegevens van andere zorginstellingen betrokken zijn

a. Is het datalek ontstaan bij HINQ of door een andere praktijk/zorginstelling gemeld aan HINQ, doorloop dan de stappen van dit protocol. Bij een datalek van gegevens die in de dossiers van de eigen praktijk/zorginstelling staan, moet de praktijk/zorginstelling altijd zelf een melding doen bij de AP, ook als het lek niet binnen de eigen praktijk/zorginstelling ontstaan is.

b. Is het datalek ontstaan in de praktijk/zorginstelling zelf en kunnen hier ook gegevens van andere zorginstellingen bij betrokken zijn? Bijv. omdat iemand onbevoegd in het systeem van de praktijk/zorginstelling heeft gekeken en ook de viewer geraadpleegd kan hebben?

   ➔ Neem dan **direct** contact op met HINQ en bepaal met HINQ welke praktijken/zorginstellingen geïnformeerd moeten worden.

   In de regionale samenwerkingsovereenkomst hebben alle deelnemers afgesproken dat de praktijk/zorginstelling:

   - de andere Partij(en) zo snel als redelijkerwijs mogelijk is, maar niet later dan 24 uur na de ontdekking van het datalek, informeren over de aard van het datalek, de mogelijke impact van het datalek op de andere Partij(en), en/ of de betrokkene(n), alsmede de maatregelen die hij heeft genomen of zal nemen om de beveiliging te corrigeren en/of de gevolgen te beperken;
   - onmiddellijk alle maatregelen nemen om de tekortkomingen in de beveiliging die hebben geleid tot het datalek te corrigeren en de gevolgen daarvan te beperken;
   - samenwerken met de andere Partij(en) om de oorzaak van het datalek te onderzoeken en alle maatregelen nemen die Partijen nodig achten om een vergelijkbaar incident te voorkomen; en
   - volledige medewerking verlenen aan het tijdig (binnen 72 uur na de ontdekking van het datalek) en adequaat informeren van de Autoriteit Persoonsgegevens en zo nodig de betrokkenen.

Contactinformatie HINQ m.b.t. datalekken

Voorzitter: Hans Niendieker, hans.niendieker@hinq.nl

Functionaris Gegevensbescherming HINQ: privacy@hinq.nl

Uitgebreidere informatie

Op de site van de Autoriteit Persoonsgegevens is uitgebreidere informatie te vinden m.b.t. datalekken:
https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken

Tips voor het voorkomen van datalekken:

- Zorg voor een goede beveiliging van de persoonsgegevens die je verwerkt.
  Let hierbij ook op de ICT-omgeving waarin gewerkt wordt. Denk bijvoorbeeld aan het opstellen van heldere procedures voor het verwerken, verzenden, archiveren of vernietigen van bestanden die persoonsgegevens bevatten.
- Stel een verantwoordelijke aan binnen de praktijk/zorginstelling.
  Dit zorgt ervoor dat verantwoordelijkheden goed zijn belegd en collega's op een laagdrempelige manier over datalekken kunnen beginnen. Zorg er wel voor dat betreffende medewerker voldoende is toegerust voor deze taak en biedt zo nodig scholing aan.
- Zorg voor goed datalekbeheer.
  Een datalekregister is verplicht, zie stap 7 van het protocol. Het is verstandig om naast de in stap 7 genoemde onderdelen ook te registeren welke afwegingen zijn gemaakt bij de beoordeling op bovenstaande vraagschema's, of het lek gemeld is aan de Autoriteit Persoonsgegevens en hoe deze datalekken in de toekomst voorkomen kunnen worden.
- Maak (nieuwe) collega's bewust van datalekken
  Werk actief met alle collega's aan de bewustwording over. Zo kunnen collega's steeds veilig werken met persoonsgegevens en vermindert het risico op datalekken.